

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-155034

(43)Date of publication of application : 14.06.1990

(51)Int.Cl.

G06F 9/06

(21)Application number : 63-308735

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 08.12.1988

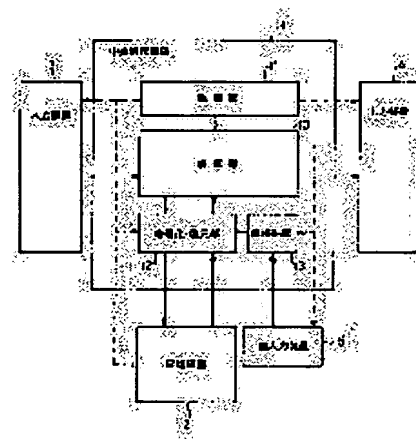
(72)Inventor : HASHIMOTO SATOSHI

(54) COMPUTER WITH SECURITY FUNCTION

(57)Abstract:

PURPOSE: To prevent the contents of a program or data from being decoded even when they leak out by providing an enciphering means and an encipherment restoring means.

CONSTITUTION: A central processing unit 1 provides an arithmetic part 10, a control part 11, an enciphering/restoring part 12, and a key storing part 13, and the program and data are stored into a storage device 2. The enciphering/restoring part 12 provides a function, which restores a value so that the arithmetic part 10 may interpret an enciphered instruction and the enciphered data on the storage device 2 with the use of a key, and a function, which enciphers the arithmetic result of the arithmetic part 10 with the use of the key at the time of writing into the storage device 2 and stores it to the storage device 2. Thus, even when the program or data in the storage device leak out, the contents of them can be prevented from being decoded, and the confidentiality of the program or the data can be improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平2-155034

⑬ Int. Cl.⁵
G 06 F 9/06

識別記号 庁内整理番号
4 5 0 B 7361-5B

⑭ 公開 平成2年(1990)6月14日

審査請求 未請求 請求項の数 1 (全7頁)

⑮ 発明の名称 セキュリティ機能付き計算機

⑯ 特 願 昭63-308735

⑰ 出 願 昭63(1988)12月8日

⑱ 発 明 者 橋 本 智 神奈川県川崎市幸区小向東芝町1 株式会社東芝総合研究
所内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑳ 代 理 人 弁 理 士 三 好 保 男 外1名

明 細 書

1. 発明の名称

セキュリティ機能付き計算機

2. 特許請求の範囲

(1) 記憶装置上の機械語命令およびデータを中央処理装置に取り込んで解釈しながら実行する計算機において、

前記中央処理装置内に設けられる格納用の格納手段と、

この格納手段に格納されている鍵を用いて前記記憶装置から暗号化された機械語命令およびデータを読み出して中央処理装置で使用可能な機械語命令およびデータに復元する暗号復元手段と、

前記格納手段に格納されている鍵を用いて前記記憶装置に格納されるデータを暗号化して前記記憶装置に格納する暗号化手段と、

を備えたことを特徴とするセキュリティ機能付き計算機。

3. 発明の詳細な説明

(発明の目的)

(産業上の利用分野)

本発明は、プログラムやデータを盗用されないようにしたセキュリティ機能付き計算機に関する。

(従来の技術)

計算機は、第10図に示すように入力装置220と、出力装置230と、中央処理装置200と、記憶装置210とを主な構成要素としている。

入力装置220及び出力装置230は、人間と計算機とのインタフェースとして使用される。

また、記憶装置210は、前記中央処理装置200を動作させるのに必要な命令、データなどからなるプログラムが格納されている。

また中央処理装置200は、計算機の制御や演算を行なう装置であり、記憶装置210からプログラムを取り込んでこれを解釈、実行する。

次に、中央処理装置200を中心として計算機の動作を説明する。

まず、中央処理装置200は、記憶装置210からプログラムを構成する命令を取り込んで、こ

れがどのような命令か解釈する。

この後、中央処理装置200はこの命令を実行し、必要があれば入力装置220から各種データや指令を取り込んだり、出力装置230から演算結果等を出力したり、記憶装置210に対してデータを格納したりする。

そして、この動作を繰り返すことにより、記憶装置210内に格納されているプログラムを実行する。

ここで、前記記憶装置210内にどのような形式で命令が格納されているかを説明する。

今、次のような即値をレジスタに格納し加算を行なうプログラムを考えてみる。

```

MOV I  REG 0, # $ 0 A B C
MOV I  REG 1, # $ 1 2 3 4
ADD    REG 0, REG 1

```

} ... (1)

上記プログラムは、アセンブリ言語で記述されたものであるが、これを中央処理装置200が解釈できるように記憶装置210上にバイナリイメージとして格納すると、次のようになる。

〔発明の構成〕

（課題を解決するための手段）

上記の目的を達成するために本発明によるセキュリティ機能付き計算機は、記憶装置上の機械語命令およびデータを中央処理装置に取り込んで解釈しながら実行する計算機において、前記中央処理装置内に設けられる鍵格納用の格納手段と、この格納手段に格納されている鍵を用いて前記記憶装置から暗号化された機械語命令およびデータを読み出して中央処理装置で使用可能な機械語命令およびデータに復元する暗号復元手段と、前記格納手段に格納されている鍵を用いて前記記憶装置に格納されるデータを暗号化して前記記憶装置に格納する暗号化手段とを備えたことを特徴としている。

（作用）

上記の構成において、記憶装置に格納されている暗号化された機械語命令およびデータを復号化手段によって復号化して中央処理装置で実行させ、また中央処理装置から記憶装置にデータを格

```

0 0 0 A B C
0 1 1 2 3 4
1 0 1 0

```

} ... (2)

（発明が解決しようとする課題）

このように通常使用されている計算機では、記憶装置210に格納される命令は、中央処理装置200に対し固有のものであり、中央処理装置200の動作と対になっている。このため、同じプログラムであれば、記憶装置210上の命令のバイナリイメージも同じになる。

したがって、中央処理装置200の命令フォーマットと命令コードとが漏洩すると、記憶装置210上のプログラムやデータの内容を秘密にすることができなくなってしまう。

本発明は上記の事情に鑑み、記憶装置内のプログラムやデータが漏洩した場合においてもその内容が解読されないようにすることができ、これによってプログラムやデータの秘匿性を高めることができるセキュリティ機能付き計算機を提供することを目的としている。

納するとき暗号化手段によって格納対象となるデータを暗号化させて格納する。

（実施例）

第1図は本発明によるセキュリティ機能付き計算機の第1実施例を示すブロック図である。

この図に示すセキュリティ機能付き計算機は、中央処理装置1と、記憶装置2と、入力装置3と出力装置4と、鍵入力装置5とを備えている。

中央処理装置1は、演算部10と、制御部11と、暗号化・復元部12と、鍵格納部13とを備えており、計算機の中心部分として機能する。

また記憶装置2は、プログラムやデータが格納される装置であり、中央処理装置1からの制御によって中央処理装置1内の暗号化・復元部12とプログラムやデータの授受を行なう。

また入力装置3及び出力装置4は、中央処理装置1からの制御で、計算機の外部からデータを受け取ったり、計算機のデータを外部に出力したりする。

また鍵入力装置5は、中央処理装置1の暗号化

や復元化を行なうのに必要な鍵をセットするために使用される装置である。

ここで、前記中央処理装置1について更に詳しく説明する。

中央処理装置1は、第1図に示す如く演算部10、制御部11、暗号化・復元部12、鍵格納部13の4つから構成されている。

演算部10は、入力装置3や記憶装置2から与えられたデータに対して算術演算や論理演算を行なう。

また制御部11は、記憶装置2からの命令を解釈し計算機全体の制御を行なう。

また暗号化・復元部12は、記憶装置2と演算部10との間にあり、暗号化されている記憶装置2上の命令及びデータを鍵を用いて演算部10が解釈できるように値を復元する機能と、演算部10で演算された結果を記憶装置2に書き込むとき鍵を用いて暗号化し記憶装置2に格納する機能とを備えている。さらに、暗号化・復元部12では、記憶装置2の内容を暗号化した命令及びデータと

して扱う場合と、暗号化した命令及びデータとして扱わない場合とを選択し得るように構成されている。

また鍵格納部13は、暗号化・復元部12で用いられる鍵が格納される部分であり、鍵入力装置5から暗号の鍵として与えられるデータを格納する機能と、命令を実行することで鍵のデータを格納する機能とを持っている。

次に、第2図ないし第4図を参照しながらこの実施例の動作を説明する。

まず、プログラムを実行するにあたって記憶装置2上に暗号化された命令及びデータを用意する。

但し、この場合に使用される暗号化プログラムは、次式に示す演算処理によって作成される。

$$Z = X1 \quad \text{x o r} \quad Y \quad \dots \dots (3)$$

但し、Z：暗号化された値。

X1：暗号化対象となる値。

Y：暗号化に用いる鍵。

この(3)式を用いて、例えば第2図に示す如くアッセンブラ(または、コンパイラなど)15

がソースプログラムを処理してバイナリイメージを出力するとき、このアッセンブラ15側にある排他的論理和手段16によって暗号化対象となるプログラムのバイナリイメージX1と、暗号化用の鍵Yとの排他的論理和をとれば、この処理結果として暗号化されたバイナリイメージZを得ることができる。このバイナリイメージZは記憶装置2に格納される。

またここで使用された鍵Yの値“1234”は、計算機でプログラムを実行させるときに用いられる鍵と同じものであり、この鍵Yをプログラム毎にユーザーあるいはOSで管理することにより計算機のセキュリティを向上させている。

次に、記憶装置2内に格納されている暗号化されたプログラムを実行する場合には、まず、鍵入力装置5から上述した暗号化処理で使用した鍵Yの値“1234”を入力する。その後、中央処理装置1にプログラムの実行開始指令を出す。

そして、この中央処理装置1が実行を開始すると、記憶装置2内にある暗号化されたプログラム

を構成する各命令が最初から順次取り込まれる。この後、この命令は第3図に示す如く暗号化・復元部12の排他的論理和手段によって次式に示す演算処理が施される。

$$X2 = Z \quad \text{x o r} \quad Y \quad \dots \dots (4)$$

但し、Z：暗号化された命令の値。

X2：復元された命令の値。

Y：暗号化に用いる鍵。

この場合、この演算によって得られる値X2は排他的論理和の性質から次式に示す如く、前記アッセンブラ15の暗号化処理対象となったバイナリイメージX1と同じである。

$$X1 = X2 \quad \dots \dots (5)$$

そして、中央処理装置1はこの処理によって得られたバイナリイメージX2を実行してプログラムされた処理を実行する。

このように、本実施例による計算機においては、記憶装置2上にある暗号化された命令及びデータを復元し、復元した値を中央装置1内部の命令として用いることで本発明の機能を持たない計算機

と同様に動作する。

またこの処理過程において、中央処理装置1から記憶装置2に処理結果などのデータを格納する必要がある場合には、第4図に示す如く暗号化・復元部12によって記憶対象となるデータのバイナリイメージX2と、暗号化用の鍵Yとの排他的論理和がとられ、この処理結果(バイナリイメージZ)が記憶装置2に格納される。

このようにこの実施例においては、鍵Yを使用しなければ、記憶装置2内に格納されている暗号化されたプログラムを処理できないようにし、かつこの暗号化されたプログラムの元プログラムを保存しないようにしたので、プログラムやデータが漏洩してもその処理内容が分からないようにすることができる。

また上述した実施例においては、暗号化・復元部12に選択機能を設け、暗号化されていないプログラムも使用し得るようにしているので、記憶装置2内に暗号化されていないプログラムが格納されているとき、このプログラムをも処理するこ

とができる。

第5図は本発明によるセキュリティ機能付き計算機の第2実施例を示すブロック図である。なおこの図において、第1図の各部と同じ部分には同じ符号が付してある。

この図に示すセキュリティ機能付き計算機が第1図に示すものと異なる点は、記憶装置2内に格納されたプログラム中に鍵Yを格納しておき、制御部11からの指令に基づいて第6図に示す如くこの鍵Yを取り出し、これを鍵格納部13に格納するようにし、暗号化されたプログラムの復元や処理結果の暗号化を行なうようにしたことである。

これによって、各プログラム毎や、プログラムの処理過程において随時、鍵Yの値を変更することができ、記憶装置2内に格納されているプログラムやデータの秘匿性をより高めることができる。

第7図は本発明によるセキュリティ機能付き計算機の第3実施例を示すブロック図である。なおこの図において、第1図の各部と同じ部分には同じ符号が付してある。

この図に示すセキュリティ機能付き計算機が第1図に示すものと異なる点は、各割込みアドレスINTADと各鍵Yとを対にして中央処理装置の演算部10c内に格納しておき、第8図に示す如く割込みがかけられたとき制御部11の制御の下に演算部10cがこの割込みに対する割込みアドレスINTADと、この割込みアドレスINTADと対になっている鍵Yを取り出し、この鍵Yを鍵格納部13に格納して、割込みアドレスINTADによって指定された暗号化プログラムの復元や処理結果の暗号化を行なうようにしたことである。

このようにすれば、各割込み処理毎に、鍵Yの値を変更することができ、記憶装置2内に格納されているプログラムやデータの秘匿性をより高めることができる。

また上述した各実施例においては、第9図に示す如く計算機によって実行される各プログラムやデータなどのアプリケーション20に鍵をかけるようにしているが、上述した各実施例と同じ手法

によってこのアプリケーション20を実行するときに使用されるOS(Operating System)21に鍵をかけるようにしても良い。

これによって、アプリケーションプログラムやデータの他に、OS21自体の秘匿性を高めることができる。

[発明の効果]

以上説明したように本発明によれば、記憶装置内のプログラムやデータが漏洩した場合においてもその内容が解読されないようにすることができ、これによってプログラムやデータの秘匿性を高めることができる。

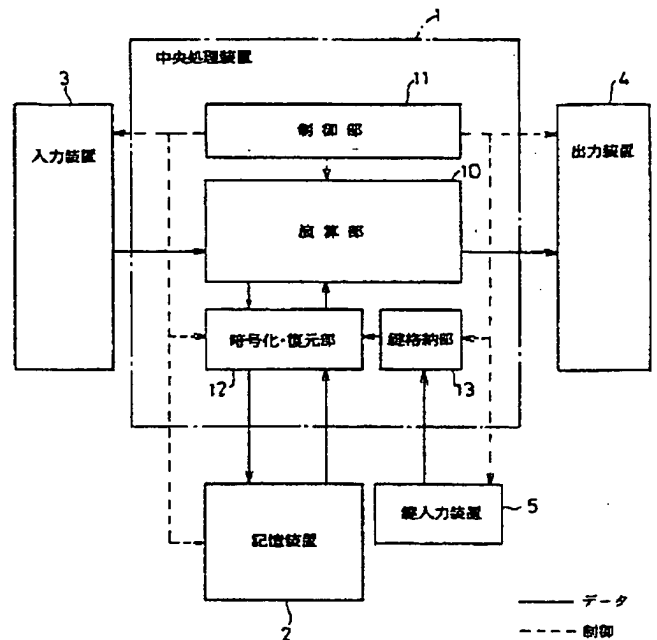
4. 図面の簡単な説明

第1図は本発明によるセキュリティ機能付き計算機の第1実施例を示すブロック図、第2図は同実施例の動作例を説明するための模式図、第3図は同実施例の動作例を説明するための模式図、第4図は同実施例の動作例を説明するための模式図、第5図は本発明によるセキュリティ機能付き計算機の第2実施例を示すブロック図、第6図は第5

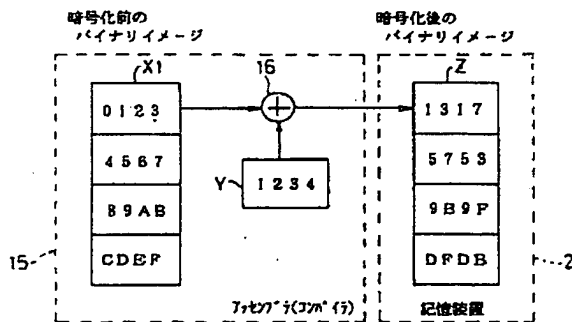
図に示す実施例の動作例を説明するための模式図、
第7図は本発明によるセキュリティ機能付き計算機
の第3実施例を示すブロック図、第8図は第7
図に示す実施例の動作例を説明するための模式図、
第9図は本発明によるセキュリティ機能付き計算
機の他の実施例を説明するための模式図、第10
図は一般的な計算機の一例を示すブロック図であ
る。

- 1 … 中央処理装置
- 2 … 記憶装置
- 12 … 暗号化手段、暗号復元手段
(暗号化・復元部)
- 13 … 格納手段 (鍵格納部)

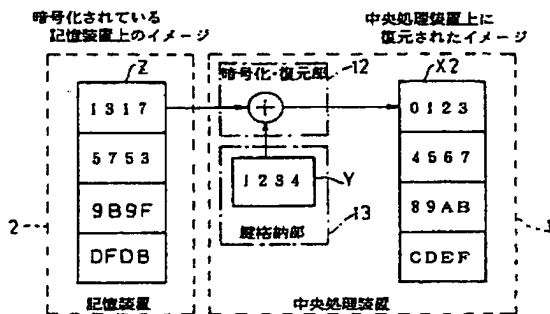
代理人 三好 保男



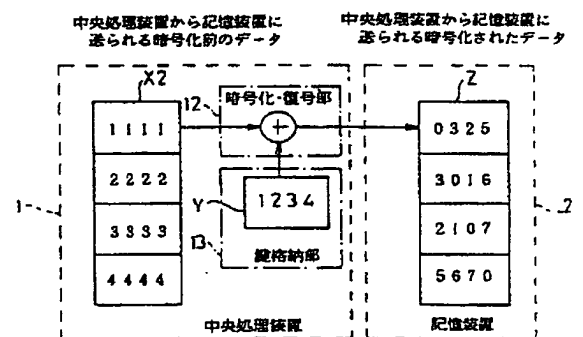
第 1 図



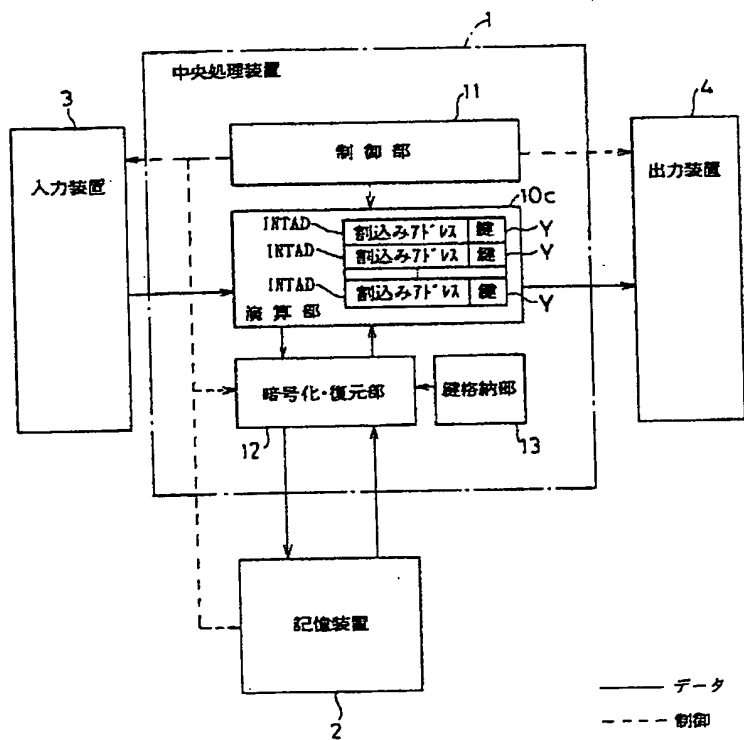
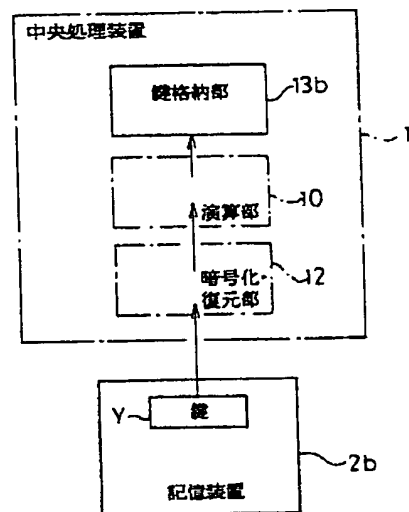
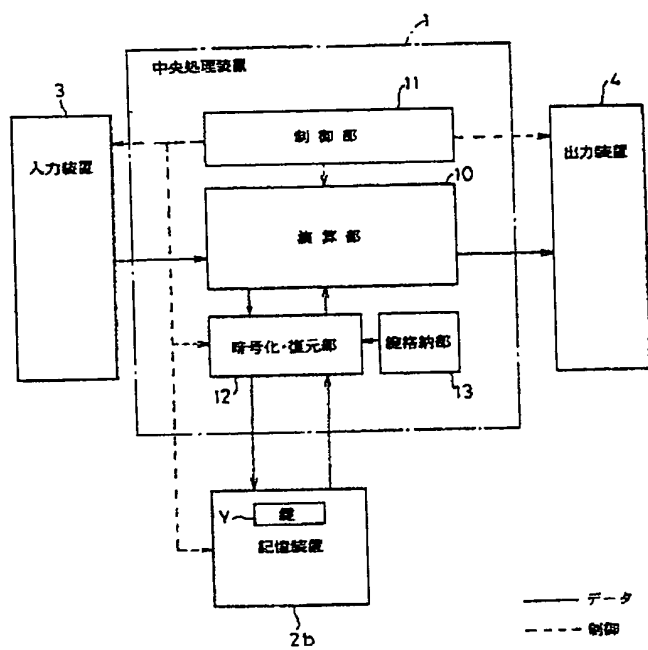
第 2 図

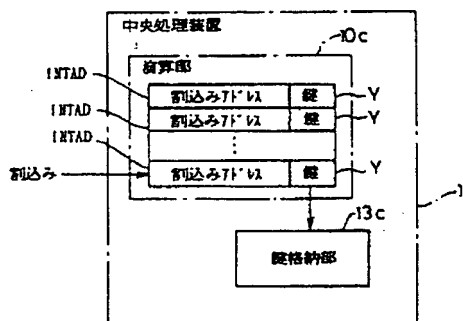


第 3 図

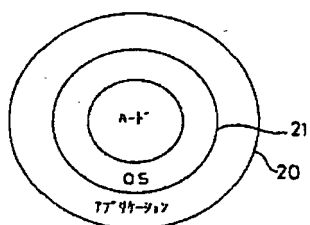


第 4 図

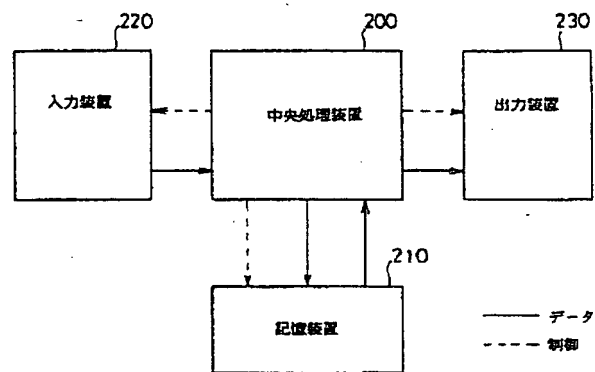




第 8 図



第 9 図



第 10 図

THIS PAGE BLANK (ISPTO)